Government of Canada / Gouvernement du Canada

Chapter 5: Handling and safeguarding of classified and protected information and assets

On this page

500. General

1. The Government of Canada is responsible for stipulating and applying the required level of security for its information and assets. These levels are Protected A, B, or C and as well as Confidential, Secret and Top Secret.

When an organization is awarded a contract that calls for safeguarding at any of these security levels, the company security officer (CSO) is responsible for consulting the appropriate government department regarding the level of security to be applied for any in-house documentation created by the organization in support of the contract. The creator of the documentation must then ensure that it is appropriately marked and safeguarded.

2. The improper handling and safeguarding of protected and classified information and assets is the leading cause of difficulties that result in the suspension or revocation of an organization's designated organization screening (DOS) or facility security clearance (FSC). The application of the procedures, detailed throughout this chapter, will help to reduce the risk of a security infraction or breach.
3. Access to information and assets must be limited to persons who have the appropriate reliability screening or security clearance **and** who have a need-to-know. Precautions must be taken to ensure that persons who are not cleared **and** who may be in the proximity of information and assets do not gain access to this information and assets.
4. Particular attention should be paid to the requirements for control and registration of information and assets and to the proper procedures for their packaging and transmittal predicated on the Policy on Government Security.
5. Additional requirements exist for the handling of communications security (COMSEC) information and assets, over and above those safeguards outlined in this chapter.

   Refer to the COMSEC (communications security) Support to the Private Sector—Project Managers' Quick Reference Guide. Contact the Contract Security Program to request a copy of this guide.

501. Security warning for contractor produced publications

1. Unless otherwise specified in the contract, where a contractor is producing a publication on behalf of the Government of Canada that contains protected information, the following warning must be printed on both the front cover and title page:

   "This publication contains PROTECTED information, which must be safeguarded under the provisions of Canada's Policy on Government Security. It has been produced by (contractor's name) under the provisions of (contract number or other

authorization) on behalf of (the Government of Canada the department, as applicable). Release of this publication or of any information contained herein to any person not authorized by the originating agency to receive it is prohibited."

2. All classified publications, pamphlets, handbooks or brochures which are produced by a contractor on behalf of the Government of Canada must have, in addition to the regular security classification markings as prescribed in this chapter, the following security warning on both the front cover and the title page:

   "This publication contains CLASSIFIED information affecting the national interest of Canada. It has been produced by (contractor's name) under the provisions of (contract number or other authorization) on behalf of (the Government of Canada or the department, as applicable) and is to be safeguarded, handled and transported in accordance with the Policy on Government Security. Release of this publication, or of any CLASSIFIED information contained herein, to any person not authorized to receive it is prohibited by the *Security of Information Act*."

3. Where a contractor produces classified publications on behalf of a foreign government department or agency, any warning must be worded as stipulated in the contractual documentation.

   You may contact international contract security to obtain further advice and assistance.

For more information, refer to the *Security of Information Act*.

502. Marking protected and classified information

General

Protected and classified information must be marked, as a minimum, according to the standards detailed in this manual.

Marking

Organizations are required to implement the following procedures for marking information:

a. for protected information, mark the word "PROTECTED" in the upper right corner of the face of the document and where required, with the letter "A", "B" or "C" to indicate the level of safeguarding

b. for Confidential information, mark the word "CONFIDENTIAL" in the upper right corner of the face of the document
c. for Secret information, mark the word "SECRET" in the upper right corner of each document page
d. for Top Secret information, mark the words "TOP SECRET" in the upper right corner of each document page and show the total number of pages on each page of the document (for example, "Page 2 of 10")
e. mark covering or transmittal letters or forms or circulation slips to show the highest level of classification or protection of the attachments
f. mark all materials used in preparing protected and classified information (such material includes notes, drafts, carbon copies and photocopies)
g. the letters used in marking should be larger than those used in the text of the document
h. printed forms that only become protected and classified when completed should be so marked, for example:

"CONFIDENTIAL"
(when completed)

i. in addition to marking individual pages as stipulated above, documents must be appropriately marked on the outside of both the front and back covers
j. loose documents must be marked on every sheet
k. images such as charts, maps and drawings must be prominently marked near the margin or title block in such manner that the marking is clearly visible when the document is folded
l. security markings should include the applicable protection or classification and the date or event at which declassification or downgrading is to occur, if it is possible to determine this at the time the information is created or collected

Marking copies

Organizations are required to implement the following procedures for controlling copies of classified information:

a. control copies of Confidential documents as for secret when warranted by a threat and risk assessment
b. for secret information, number each copy, show the copy number on the face of each copy and maintain a distribution list
c. for top secret information, assign a unique whole number to each copy, marking the copy number on each page and maintain a distribution list. Recipients of top secret

- information must not copy it without specific authorization of the Canadian Industrial Security Directorate (CISD)

Marking microforms

a. Microform is a generic term for any storage medium that contains micro-images
b. Organizations are required to implement the following procedures for the marking of microforms:
    a. assign a protection or security classification at the highest protection or classification of the information contained on the microform
    b. mark microforms containing protected information "PROTECTED" in eye-readable form, with the microform number and the total number of microforms
    c. mark microforms containing classified information with the proper classification in eye-readable form, with the microform number and the total number of microforms

Marking electronic storage material

a. Electronic material on which is stored protected and classified information is to be assigned a protection and security classification at the highest protection or classification of the information it contains.
b. Where possible, the security marking should be in both eye-readable and machine-readable form. Where this is not possible, as with certain types of hard disks, the security marking should be machine-readable.
c. Electronic storage material includes flexible disks, hard disks (both removable and permanent), storage cartridges, printed output from computers, video display units, magnetic tapes, magnetic cassettes, punched cards and punched paper tapes.
d. Removable storage material should bear standard labels. Where bypass label processing is allowed, procedures are needed to ensure that the proper item is loaded into the computer.

    Refer to Chapter 8: Information Technology Security of this manual.

e. Specific advice on how to mark various forms of electronic storage material may be obtained from CISD (Canadian Industrial Security Directorate).

International documentation

Marking must be in accordance with international industrial security memoranda of understanding, agreements or other international standards and guidelines.

You may contact international contract security to obtain further advice and assistance.

503. Records management

General

Organizations must maintain records and establish adequate facilities, such as a records office, for receiving, distributing and storing protected and classified information and assets.

Recording of protected information and assets

Unless specifically identified in a contract, there is no requirement to keep records of protected information and assets, except for Protected C, which must be recorded in the same manner as classified information and assets. Persons receiving or granted access to protected information and assets must be briefed on their responsibilities for its safeguarding.

Recording of classified information and assets

A record must be kept of the dates, names and transactions of all classified information and assets indicating:

a. receipt by the facility
b. distribution within the facility
c. creation within the facility
d. reproduction within the facility
e. destruction within the facility
f. transmittal outside the facility
    - Transmittal of information and assets outside the facility must be performed as detailed in section 506. Packaging and transmittal of classified and protected information and assets of this chapter. Records of distribution, circulation and return within the facility must include receipt by signature, of the persons involved. Persons who have access to classified information and assets must be briefed on their responsibilities for its protection, and any special restrictions concerning its use or further dissemination
g. All records of classified information and assets **and all classified information and assets** must be made available for inspection by field industrial security officers of CISD (Canadian Industrial Security Directorate)

Records office security

Management of records offices, or parts thereof, where protected and classified information is stored or processed must ensure the following procedures are followed:

a. as a minimum, these offices must be managed as a security zone
b. records office staff who have access to protected and classified information must hold a reliability status or personnel security clearance to the highest level required
c. protected and classified information must be filed and circulated in marked file jackets that clearly indicate they contain protected and classified information
d. a file must be marked according to the highest level of sensitivity retained in the file
e. areas where mail is opened must be managed according to mailroom security standards. Refer to the section on Mailroom security below
f. release of protected files from records offices must be limited to employees with reliability status with a need-to-know
g. release of confidential files from records offices must be limited to security-cleared employees with a need-to-know
h. release of top secret and secret files from records offices must be limited to appropriately security-cleared employees with a need-to-know. Those personnel authorized access must be identified on an access list approved by the responsible manager (such as the project manager)
i. classified information of foreign origin must be accorded the same protection as Canadian information of equivalent classification. If in doubt, contact international contract security to obtain further advice and assistance
j. special precautions are necessary to prevent unauthorized disclosure or access to classified information and assets to non-Canadian citizens:
    - such persons must not be given access to information that bears restrictive markings such as "FOR CANADIAN EYES ONLY" without prior approval of CISD (Canadian Industrial Security Directorate)
    - further restrictions may apply to bilateral and multinational contracts, programs or projects. If in doubt, contact CISD (Canadian Industrial Security Directorate)

Mailroom security

Areas where mail is opened must be managed as a security zone or high-security zone. Mail that is marked "to be opened only by the addressee" must be delivered to the intended recipient directly. Classified mail must only be opened by the appointed authority within the facility responsible for ensuring its registration.

504. Safeguarding of information and assets

Storage

a. As a minimum, protected information and assets must be stored in a locked container. Protected C information and assets and all classified information must be stored in an approved security container in accordance with the Royal Canadian Mounted Police (RCMP) Technical Security Branch Security Equipment Guide (G1-001). Protected or classified information and assets may be stored on open shelving in a secure room, only after inspection and approval by CISD (Canadian Industrial Security Directorate) and only to the level approved by CISD (Canadian Industrial Security Directorate).

b. Protected and classified information and assets must not be stored in the same container as negotiable or attractive assets.

c. Organizations required to store protected and classified information and assets are permitted to purchase approved security equipment through Public Services and Procurement Canada. In consultation with the field industrial security officer, the CSO (company security officer) or alternate company security officer (ACSO) should determine the equipment to meet the specific requirement, and submit the Annex 5-A: Registering a document for equipment purchase form in this chapter. After endorsement by the field industrial security officer, Public Services and Procurement Canada will process the request, although the invoicing and delivery for the equipment is between the purchaser (the CSO (company security officer)) and the supplier. Examples of equipment available through this procedure are listed in Annex 5-B: Approved equipment available for purchase by organizations.

Keys for containers

a. Keys (devices such as instruments, cards, combinations and code numbers used to open and close containers) must be safeguarded at the highest level of sensitivity of the information or assets to which they provide access. This also applies to recorded information that would allow a key to be produced.

b. When a key is issued, the recipient must sign for the key. The number of the key, the location of the container it opens, and the name of the recipient must be recorded and kept by the CSO (company security officer).

c. The organization's security office must maintain a record of the dates of, and reasons for, all key changes.

d. Assigned keys should be changed:

   1. at least every 12 months

2. when those with access to the container are transferred, released or no longer require access

The key **must** be changed immediately when a container has been or may have been compromised.

Precautions during use

Special care must be taken to safeguard against disclosure or unauthorized access when protected and classified information and assets are removed from approved storage containers. Specific points to observe are:

a. do not leave protected and classified information and assets unattended
b. ensure that protected and classified information and assets cannot be viewed, or discussion of it overheard, by persons not possessing reliability screening or the appropriate level of clearance or without a need-to-know

505. Use of laptop computers

1. If laptop computers are utilized for protected or classified information, they **must not** be removed from the organization that holds the facility security clearance (FSC) or designated organization screening (DOS). If such laptops need to be transported, written permission must be obtained from the CSO (company security officer) or an ACSO (alternate company security officer) by completing the Annex 5-D: Appendix A-1-Courier certificate/itinerary form.
2. Storage of laptop computers used to handle protected or classified information must be in accordance with security procedures established by the organization for the level of sensitivity of the information.

506. Packaging and transmittal of classified and protected information and assets

1. The security of protected and classified information and assets during transmission depends on:
   a. proper packaging
   b. record while in transit
   c. record of delivery

d. transmission by an approved postal service or security-cleared courier. Contact international contract security regarding approved postal services and security-cleared couriers

2. Protected and classified information and assets must be packaged and transmitted in accordance with the standards outlined in Annex 5-C: Standard for the transmittal of classified and protected information and assets.
3. In addition, specific procedures for the hand carriage of and/or bulk shipment of specific protected and classified information and assets are necessary. These procedures are detailed in the following annexes and appendices:

   - Annex 5-A: Registering a document for equipment purchase form
   - Annex 5-B: Approved equipment available for purchase by organizations
   - Annex 5-C: Standard for the transmittal of classified and protected information and assets
   - Annex 5-D: Arrangement for the hand carriage of classified/Protected B documents, equipment and/or components within Canada
     - Annex 5-D: Appendix A-1—Courier certificate/itinerary form
     - Annex 5-D: Appendix A-2—Notes for the courier
     - Annex 5-D: Appendix A-3—Pre-trip declaration form
     - Annex 5-D: Appendix A-4—Post-trip declaration form
   - Annex 5-E: Arrangements for escorting Secret, Confidential or Protected C bulk shipments within Canada that cannot be hand carried
     - Annex 5-E: Appendix A-1—Courier certificate/itinerary form
     - Annex 5-E: Appendix A-2—Notes for the escort
     - Annex 5-E: Appendix A-3—Pre-trip declaration form
     - Annex 5-E: Appendix A-4—Post-trip declaration form

507. Temporary removal of classified and protected information and assets

1. Protected and classified information and assets cannot be removed from an organization, for transportation or use outside of Canada, without the prior approval of CISD (Canadian Industrial Security Directorate).
2. In Canada, with the exception of Top Secret, Protected C and COMSEC (communications security) material, protected and classified information and assets may be taken temporarily from an organization. Written permission must be obtained from the CSO (company security officer) or an authorized ACSO (alternate company

security officer) by completing the Annex 5-D: Appendix A-1—Courier certificate/itinerary form.

3. The CSO (company security officer) or ACSO (alternate company security officer) must record, and obtain a receipt for the information and assets to be removed.
4. If protected and classified information and asset removal is authorized for overnight use, the employee must be informed that this does not constitute continued retention authority and the information and assets are to remain in the possession of the employee at all times.
5. The CSO (company security officer) or ACSO (alternate company security officer) must account for and record the material upon its return, and give the employee a receipt for the returned material.

508. Reproduction

1. Reproductions of protected information must be marked in the same manner as the originals. Reproduction of classified information must only be done with the authorization of the CSO (company security officer), or an authorized ACSO (alternate company security officer). Reproductions must be marked, registered and accounted for, in the same manner as for the originals.
2. Some classified information bears a caveat prohibiting or restricting reproduction. In such cases, authorization of the originator is required before reproduction. Protected C, Top Secret, and COMSEC (communications security) information must **never** be reproduced without written authorization from CISD (Canadian Industrial Security Directorate).
3. Special precautions must be taken with the use of photocopy machines. Notices concerning the proper procedures for reproduction of information must be placed in an obvious place close to each machine. Care should be taken to ensure that original documents are not left in the machine, and all copies, including waste, are removed.
4. Contracts for printing and microfiching of protected and classified documents must only be awarded to commercial firms that have the appropriate level of DOS (designated organization screening) or FSC (facility security clearance).

509. Reclassification and declassification

1. Documents whose classification markings include a schedule for downgrading or declassification may be downgraded or declassified in accordance with the schedule, unless in receipt of notification to the contrary. Documentation that does not contain

such provisions may only be downgraded or declassified upon receipt of written authorization from the originator through CISD (Canadian Industrial Security Directorate).

2. When an organization considers that foreign or North Atlantic Treaty Organization (NATO) classified information should be downgraded or declassified, it must submit a written request to international contract security with full details, including justification.
3. When official notification is received from CISD (Canadian Industrial Security Directorate) authorizing the reclassification of a document, all copies must be re-marked with the new classification as follows:

Declassified
or
Downgraded to (insert new classification)
or
Upgraded to (insert new classification)
by authority of Public Services and Procurement Canada letter dated (insert date)
or
by authority of Security Requirements Checklist dated (insert date)
or
by authority of contract dated (insert date)

510. Retention

1. When a bid is not accepted, or upon completion or termination of the contract, protected and classified material and assets must be returned to CISD (Canadian Industrial Security Directorate) for disposal or, with the written concurrence of CISD (Canadian Industrial Security Directorate), be destroyed by the organization or returned to the originator. Upon request, organizations may be authorized to retain such material when approved by the originator through CISD (Canadian Industrial Security Directorate).
2. Requests for retention authority must identify:
   - the material for which retention is requested
   - the period for which retention will be required
   - the justification for retention

   If the organization has been authorized to retain protected and classified information for a specific period after contract completion, details of this authorization must be included with the retention request.

3. Unless the retention authority is received in writing, disposal of protected and classified information must be made in accordance with the provisions of this manual and instructions from CISD (Canadian Industrial Security Directorate).

511. Destruction

1. Unless otherwise specified, Protected C, Top Secret, COMSEC (communications security) and foreign classified information and assets must be returned to CISD (Canadian Industrial Security Directorate) for disposal.
2. Unless otherwise specified, Protected A and B, Secret and Confidential information and assets, of Canadian origin, may be destroyed by the organization with the approval of CISD (Canadian Industrial Security Directorate).

   Note: Destruction of classified information and assets must be recorded on a certificate of destruction form, a copy of which must be forwarded to the Document Control Unit at CISD (Canadian Industrial Security Directorate).

3. Protected and classified information and assets that have been authorized for destruction must be disposed of in accordance with the following:
   a. it must be destroyed only by approved destruction equipment, or at a facility authorized by CISD (Canadian Industrial Security Directorate)
   b. information awaiting destruction or in transit to destruction must be safeguarded in the manner prescribed for the most highly protected and classified information asset involved
   c. protected and classified information and assets awaiting destruction must be kept separate from other information and assets awaiting destruction
   d. an employee with a reliability status or with a proper security clearance, as applicable, must be present to monitor the destruction of protected and classified information respectively
   e. surplus copies and waste that could reveal protected and classified and information must be protected to the appropriate level and should be promptly destroyed

512. Security violations, breaches, and compromises

1. Organizations must establish a procedure to ensure that suspected or actual violations of security, breaches and compromises are recorded and immediately reported to the CSO (company security officer). Records should be kept by the

organization for a period of 2 years following the incident and are subject to inspection by the field industrial security officer.

2. Upon receipt of such a report, the CSO (company security officer) must immediately conduct a preliminary inquiry into the incident to determine all of the circumstances, including:
   a. What, where and when did the incident occur?
   b. Who reported it, to whom, and when?
   c. What information or asset was involved (in detail)?
   d. What was the security marking and description of the information or asset involved?
   e. Who originated the information or asset?
   f. When, for how long, and under what circumstances was the information or asset vulnerable to unauthorized disclosure, and to whom?
   g. What actions were taken to secure the information or asset and limit the damage?
   h. Is any information or asset lost or unaccounted for?
3. When the results of the preliminary inquiry indicate a suspected or actual breach or compromise of information and assets, CISD (Canadian Industrial Security Directorate) is to be immediately notified by the CSO (company security officer). A full report covering the preliminary inquiry and any subsequent investigative results are to be forwarded to CISD (Canadian Industrial Security Directorate) as soon as possible.

513. Verbal and message communication

1. Unprotected telephones or facsimiles are not to be used to communicate classified or sensitive information. Requirements for secure telephones or facsimiles must be coordinated through the Communications Security Establishment (CSE).
2. Any conference rooms used for discussion of classified matters should be:
   a. a sensitive discussion area located in a security zone or high-security zone
   b. safeguarded against acoustic or electronic eavesdropping and should not contain items such as:
      i. telephones
      ii. intercoms
      iii. radios
      iv. tape recorders

Annexes

- Annex 5-A: Registering a document for equipment purchase form
- Annex 5-B: Approved equipment available for purchase by organizations
- Annex 5-C: Standard for the transmittal of classified and protected information and assets
- Annex 5-D: Arrangement for the hand carriage of classified/Protected B documents, equipment and/or components within Canada
  - Annex 5-D: Appendix A-1—Courier certificate/itinerary form
  - Annex 5-D: Appendix A-2—Notes for the courier
  - Annex 5-D: Appendix A-3—Pre-trip declaration form
  - Annex 5-D: Appendix A-4—Post-trip declaration form
- Annex 5-E: Arrangements for escorting Secret, Confidential or Protected C bulk shipments within Canada that cannot be hand carried
  - Annex 5-E: Appendix A-1—Courier certificate/itinerary form
  - Annex 5-E: Appendix A-2—Notes for the escort
  - Annex 5-E: Appendix A-3—Pre-trip declaration form
  - Annex 5-E: Appendix A-4—Post-trip declaration form

Date modified:

2018-12-05